UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,150	05/14/1999	PHILIP J. MIRE	M-7219-US	2203

7590 06/06/2003

DAVID L. McCOMBS
HAYNES and BOONE, LLP
901 MAIN STREET
SUITE 3100
DALLAS,, TX 75202-3789

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/312,150	MIRE, PHILIP J.
	Examiner	Art Unit
	Aravind K Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☒ Claim(s) *6 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 May 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Public Key Infrastructure Utilizing Master Key Encryption.

Drawings

2. The drawings are objected to reasons as stated in form PTO 948.

Claim Objections

3. Claims 6 and 17 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 6 and 17 depend on claims 1 and 12. Claims 1 and 12 recite the limitation "encrypting the session key utilizing a user's public key". By reciting, "encrypting the session key utilizing the user's public key" in claims 6 and 17, it does not further limit the limitation in claims 1 and 12.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-8, 12-19 and 23-28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 in view of Applied Cryptography (hereinafter Schneier).

As to claim 1, Burke discloses a method for encrypting data. Burke discloses generating a session key [abstract]. Burke discloses encrypting the data utilizing the session key [column 4, lines 35-37]. Burke discloses encrypting the session key utilizing a user's key [column 5, lines 22-25]. Burke discloses encrypting the session key utilizing a master key [column 5, lines 17-20]. Burke discloses generating a data packet including the encrypted data and the encrypted session keys [column 5, lines 13-32].

Burke is silent as to the type of the user and master key.

Schneier teaches public-key management and its benefits [pages 185-187].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burke so that the master key and the user's key were both public keys. The keys included in the data packet would have been encrypted with a user public key and a master public key.

The motivation to modify Burke by the teaching of Schneier would have been that a private key of the public-private key pair authenticates a relationship as well as an identity [page 186].

As to claim 2, the Burke-Schneier combination teaches transmitting the data packet to a destination data processing system [Burke column 5, lines 33-41]. Burke teaches decrypting the session key [column 5, lines 33-36]. The examiner asserts that if the session key was encrypted with the user's public key as taught by Schneier then the only key that can decrypt the session

key is the private key. The Burke-Schneier combination teaches decrypting the data utilizing the session key [Burke column 5, lines 50-51].

As to claim 3, the Burke-Schneier combination teaches decrypting the encrypted session key with a master private key. Burke teaches decrypting the session key with the master key [column 5, lines 43-48]. The examiner asserts that if the session key was encrypted with the public key (master) as taught by Schneier then the only key that can decrypt the session key is the private key (master). The Burke-Schneier combination teaches decrypting the data with the session key [Burke column 5, lines 50-51].

As to claim 4, the Burke-Schneier combination teaches encrypting the session key utilizing an asymmetric encryption routine. Schneier teaches that public-key cryptography is also called asymmetric algorithms [page 4].

As to claim 5, the Burke-Schneier combination teaches encrypting the data utilizing a symmetric encryption routine. Schneier teaches that symmetric algorithms have the same encryption key and decryption key [page 4]. The examiner asserts that since the same session key is used to encrypt and decrypt data, as taught by Burke, thus symmetric encryption is being utilized.

As to claim 6, the Burke-Schneier combination teaches encrypting the session key utilizing the user's public key, as discussed above.

As to claim 7, the Burke-Schneier combination teaches storing the user's private key on a storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al]. The examiner

asserts that since public-key encryption was being used the user's private key has to be stored at the destination processing system in order to decrypt the session key.

As to claim 8, the Burke-Schneier combination teaches storing the master private key on a data storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al].

As to claim 12, Burke discloses a method for encrypting data. Burke discloses generating a session key [abstract]. Burke discloses encrypting the data utilizing the session key [column 4, lines 35-37]. Burke discloses encrypting the session key utilizing a user's key [column 5, lines 22-25]. Burke discloses encrypting the session key utilizing a master key [column 5, lines 17-20]. Burke discloses generating a data packet including the encrypted data and the encrypted session keys [column 5, lines 13-32].

Burke is silent as to the type of the user and master key. Burke does not teach a certificate containing data pertaining to the user including the user's public key.

Schneier teaches public-key management and its benefits. Schneier teaches certificates that contain data pertaining to the user and including the user's public key [pages 185-187].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burke so that the master key and the user's key were both public keys. The keys included in the data packet would have been encrypted with a user public key and a master public key. There would also have been a certificate that contained data pertaining to the user and including the user's public key.

The motivation to modify Burke by the teaching of Schneier would have been that a private key of the public-private key pair authenticates a relationship as well as an identity [page 186].

As to claim 13, the Burke-Schneier combination teaches transmitting the data packet to a destination data processing system [Burke column 5, lines 33-41]. Burke teaches decrypting the session key [column 5, lines 33-36]. The examiner asserts that if the session key was encrypted with the user's public key as taught by Schneier then the only key that can decrypt the session key is the private key. The Burke-Schneier combination teaches decrypting the data utilizing the session key [Burke column 5, lines 50-51].

As to claim 14, the Burke-Schneier combination teaches decrypting the encrypted session key with a master private key. Burke teaches decrypting the session key with the master key [column 5, lines 43-48]. The examiner asserts that if the session key was encrypted with the public key (master) as taught by Schneier then the only key that can decrypt the session key is the private key (master). The Burke-Schneier combination teaches decrypting the data with the session key [Burke column 5, lines 50-51].

As to claim 15, the Burke-Schneier combination teaches encrypting the session key utilizing an asymmetric encryption routine. Schneier teaches that public-key cryptography is also called asymmetric algorithms [page 4].

As to claim 16, the Burke-Schneier combination teaches encrypting the data utilizing a symmetric encryption routine. Schneier teaches that symmetric algorithms have the same encryption key and decryption key [page 4]. The examiner asserts that since the same session

key is used to encrypt and decrypt data, as taught by Burke, thus symmetric encryption is being utilized.

As to claim 17, the Burke-Schneier combination teaches encrypting the session key utilizing the user's public key, as discussed above.

As to claim 18, the Burke-Schneier combination teaches storing the user's private key on a storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al]. The examiner asserts that since public-key encryption was being used the user's private key has to be stored at the destination processing system in order to decrypt the session key.

As to claim 19, the Burke-Schneier combination teaches storing the master private key on a data storage medium coupled to the destination data processing system [element **11** of figure 1 of Lennon et al U.S. Patent No. 4,193,131 incorporated by reference to Burke et al].

As to claim 23, Burke discloses a method for encrypting data and decrypting data. Burke discloses generating a session key [abstract]. Burke discloses encrypting the data utilizing the session key [column 4, lines 35-37]. Burke discloses encrypting the session key utilizing a user's key [column 5, lines 22-25]. Burke discloses encrypting the session key utilizing a master key [column 5, lines 17-20]. Burke discloses generating a data packet including the encrypted data and the encrypted session keys [column 5, lines 13-32].

Burke is silent as to the type of the user and master key.

Schneier teaches public-key management and its benefits [pages 185-187].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burke so that the master key and the user's key were both

public keys. The keys included in the data packet would have been encrypted with a user public key and a master public key. The examiner asserts that encrypting and decrypting takes place on a computer that its inherent that it would have been implemented on a computer usable medium having computer readable code embodied therein.

The motivation to modify Burke by the teaching of Schneier would have been that a private key of the public-private key pair authenticates a relationship as well as an identity [page 186].

As to claim 24, the Burke-Schneier combination teaches transmitting the data packet to a destination data processing system [Burke column 5, lines 33-41]. Burke teaches decrypting the session key [column 5, lines 33-36]. The examiner asserts that if the session key was encrypted with the user's public key as taught by Schneier then the only key that can decrypt the session key is the private key. The Burke-Schneier combination teaches decrypting the data utilizing the session key [Burke column 5, lines 50-51].

As to claim 25, the Burke-Schneier combination teaches decrypting the encrypted session key with a master private key. Burke teaches decrypting the session key with the master key [column 5, lines 43-48]. The examiner asserts that if the session key was encrypted with the public key (master) as taught by Schneier then the only key that can decrypt the session key is the private key (master). The Burke-Schneier combination teaches decrypting the data with the session key [Burke column 5, lines 50-51].

As to claim 26, the Burke-Schneier combination teaches encrypting the session key utilizing an asymmetric encryption routine. Schneier teaches that public-key cryptography is also called asymmetric algorithms [page 4].

As to claim 27, the Burke-Schneier combination teaches encrypting the data utilizing a symmetric encryption routine. Schneier teaches that symmetric algorithms have the same encryption key and decryption key [page 4]. The examiner asserts that since the same session key is used to encrypt and decrypt data, as taught by Burke, thus symmetric encryption is being utilized.

As to claim 28, the Burke-Schneier combination teaches encrypting the session key utilizing the user's public key, as discussed above.

5. Claims 9, 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 and Schneier as applied to claim 1 above, and further in view of Dillaway et al U.S. Patent No. 5,742,756.

As to claim 9, the Burke-Schneier combination does not teach retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the user's private key is stored on a smart card coupled to the destination node. The private key is only retrieved when the smart card is inserted into the smart card reader.

The motivation to have modified the Burke-Schneier combination by the teaching of Dillaway is in using a smart Card to perform critical cryptography operations. The smart Card can be programmed or otherwise configured to never expose the user's private keys. Rather than

providing a private key to the user's computer, the key is held within the smart Card, and required cryptographic operations are performed on the smart Card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claim 10, the Burke-Schneier combination does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

The motivation to have modified the Burke-Schneier combination by the teaching of Dillaway is in using a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claim 20, the Burke-Schneier combination does not teach retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system, figure 2.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the user's private key is stored on a smart card coupled to the destination node. The private key is only retrieved when the smart card is inserted into the smart card reader.

The motivation to have modified the Burke-Schneier combination by the teaching of Dillaway is in using a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claim 21, the Burke-Schneier combination does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system, figure 2.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

The motivation to have modified the Burke-Schneier combination by the teaching of Dillaway is in using a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

6. Claims 11, 22 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burke et al U.S. Patent No. 5,706,347 and Schneier as applied to claims 1 and 23 above, and further in view of Kruys U.S. Patent No. 5,555,309.

As to claims 11 and 29, the Burke-Schneier combination does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

The motivation to have modified the Burke-Schneier combination by the teaching of Kruys is that master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

As to claim 22, the Burke-Schneier combination teaches decrypting the data with the session key, as discussed above.

The Burke-Schneier combination does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

The motivation to have modified the Burke-Schneier combination by the teaching of Kruys is that master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail O Hayes can be reached on 703-305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

May 22, 2003

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100